DEPARTMENT OF ADMINISTRATIVE SERVICES
INTERNAL POLICIES AND PROCEDURES

330 **Data Incident Response**

Effective: July 1, 2015
Revised: October 26, 2020
Reviewed: October 26, 2020

References:

Purpose:

The purpose of this policy is to establish a protocol for the response of a Department of Administrative Services (DAS) Information Technology (IT) incident or event, which impacts computing equipment, data, mobile devices, or networks.

Definitions:

1. *Agency Response Team (ART):* The Department's response team will consist of at least the following: Department Security Officer, the Department of Technology Services (DTS) IT director assigned to DAS, the DAS Public Information Officer (PIO), and the Division Director experiencing the incident. The ART team will report directly to the DAS Executive Director.

2. *Breach:* The unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by DAS.

3. *Computer Security Incident:* An act or circumstance in which there is a deviation from the requirements of security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents, including any unauthorized activity that threatens the confidentiality, integrity or availability of state information system resources.

4. *Information Systems:* Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog): includes software, firmware, and hardware.

5. *Intruder:* Hacker, botnet, malware, etc. Intruder may also include an authorized system user accessing data in an inappropriate manner or for inappropriate usage.

6. *Personally Identifiable Information (PII):* Any piece of information that can potentially be used to uniquely identify, contact, or locate a single person. Data that provides personal or private information that should not be publicly available. For example, personally identifiable information could be an individual's Social Security Number (SSN), name or address in conjunction with one of more of the following: date of birth, SSN, tax

identification number, or equivalent, financial account number, and credit or debit card number.

Policy:

1. Prioritization

An incident is prioritized based on the following:

- Current and potential effect of the incident (breach, public concern, data destruction, root compromise)
- Criticality of the affected resource (web server, public accessible application, critical agency resource)

The combined criticality of the potential effect of the incident combined with the criticality of the affected resource determines the impact of the incident – for example, the loss of an encrypted data storage device with non-private data might result in a minor loss of productivity, whereas, root compromise of an application server where restricted data is hosted might result in a loss of data, harm to the public, and damage to the DAS reputation.

2. Incident Reporting

Each computer security incident, including suspicious events, shall be reported immediately (orally or via email) to the employee's supervisor and to the DAS Security Officer by the employee who witnessed/identified the incident.

The DAS Security Officer shall determine the criticality of the incident. If the incident is determined to have a potentially serious impact, the Security Officer will assemble and brief the ART. If the DTS IT Director is unavailable, the DAS Security Officer will contact the State Security Officer directly.

The ART will determine if other agencies, divisions, or personnel need to become involved in the resolution of the incident. Only the Executive Director, the Executive Director's designee, or the DAS PIO will speak to the press about an incident.

3. Mitigation and Containment

Any system network, or security administrator who observes an intruder on a State of Utah network or system shall take appropriate action to immediately terminate the intruder's access. Affected systems, such as those infected with malicious code or systems accessed by an intruder shall be isolated from the network until the damage can be assessed. Any discovered vulnerabilities in the network or system will be rectified by appropriate means as soon as possible and in accordance with DTS policy.

4. Information Dissemination

Any public release of information concerning a computer security incident shall be coordinated by the DAS PIO. The DAS PIO shall manage the dissemination of incident information to other participants, such as law enforcement or other incident response agencies. The DAS PIO shall coordinate dissemination of information that could affect the public, such as web page defacement or situations that disrupt systems or applications.